J Fail. Anal. and Preven.
https://doi.org/10.1007/s11668-020-00967-x

TECHNICAL ARTICLE—PEER-REVIEWED

Failure Mode Investigation and Redundancy Management of an Electromechanical Control Actuator for Launch Vehicle Application

B. Biju Prasad · N. Biju · M. R. Radhakrishna Panicker · K. Kumar · V. Murugesan

Submitted: 19 May 2020

Abstract Electromechanical actuators (EMAs) are increasingly being used in aircrafts under the *More Electric Aircraft* initiatives. New satellite launch vehicles are being configured with EMA for the thrust vector control and mixture ratio control systems. Analysis of failure modes and their effects in the design stage of a new system is an essential exercise to be done for safety–critical applications of aircraft and human-rated launch vehicle. The thrust vector control system used in the terminal stage of a satellite launch vehicle which does not have any fault tolerance, referred hereafter as no redundancy actuator (NRA), is considered for the case study. At first, a thorough study is conducted on the failures encountered in the NRA and the corrective actions to be taken to avoid these failures in the new design are identified. Improvement in fault tolerance is attempted in two phases. In the first phase, the redundancy features are incorporated in the electrical systems of the actuator such as electric motors and sensors which form part of the closed loop system, leading to the electrical redundancy actuator (ERA). The next logical step is to use a high redundancy actuator (HRA) having fault tolerance to stuck and loose failures in its moving elements such as ball bearings, ball screws and motors. In this paper, failure mode and effects analysis (FMEA) of the existing and the two proposed configurations is carried out. The HRA is designed following the failure mode avoidance technique through four strategies, which are relaxing a constraint limit, using physics of incipient failure, having different operating modes and exploiting dependencies among failure modes. It is concluded that the HRA configuration eliminates a number of single failure points present in NRA and ERA, and it is found to have a better fault tolerance to the failures in its electrical and mechanical elements.

Keywords FMEA · Thrust vector control · Electromechanical actuator · Motor · Ball screw · Bearing

B. Biju Prasad (✉) · N. Biju · M. R. Radhakrishna Panicker
School of Engineering, Cochin University of Science & Technology, Kochi, India
e-mail: bijuprasadb@yahoo.com; bijuprasadb@gmail.com

K. Kumar · V. Murugesan
Vikram Sarabhai Space Center, Trivandrum, India

Introduction

Rapid advancement is happening in aircrafts under the *More Electric Aircraft* initiatives to improve the maintainability, reliability and maneuverability of future aircrafts [1]. Consequent to the invention of high-energy rare earth magnets and the tremendous advancement in high power electronics and lithium-ion batteries, EMA systems are replacing the conventional hydraulic systems for launch vehicles and more electric aircrafts. They find application in automatic control systems for ground-based and aerospace applications. EMAs have lot of advantages owing to its simple designs over the conventional hydraulic systems which have complex mechanical system configuration with a more number of subsystems and susceptibility for failures due to leaks, pressure drop, contamination and lower storage life. Actuators are used in satellite launch vehicle for the thrust vector control and mixture ratio control of fuel and oxidizer. Control and guidance function of the launch vehicle is achieved through the thrust vector control by deflecting the exhaust jet. Typically, the engine or nozzle is moved to deflect the thrust in the thrust vector

Published online: 18 August 2020

control system or by injecting a high-density fluid into the exhaust jet named as secondary injection thrust vector control method. Two rotary actuators are positioned close to the gimbal bearing for smaller engines and two linear actuators are positioned orthogonally in bigger engines for the pitch and yaw control of the vehicle. There is a need to improve the reliability of control actuation system in human-rated vehicles and in satellite launch vehicles carrying out advanced and costly missions. Incorporating redundancy to the critical elements is one of the methods to improve the system reliability. The traditional approach is to provide redundancy to the electrical elements such as sensors, motor windings, drive circuits and controllers. In such cases, there is a need for the fault detection, isolation and recovery (FDIR) of such systems. Hence, FDIR of electromechanical control actuation systems has been an active research topic in recent times. This deals with the monitoring of a system, identifying a fault when it occurs and locating and categorizing it. Model-based FDI and signal processing-based FDI are two approaches that are commonly used to handle the fault. Each approach has its own merits and demerits in terms of the severity of the anticipated failures, the probability of occurrence of failures and the ability to detect each of the failure modes. Hence, it is important to conduct a failure mode and effects analysis (FMEA) in the design stage itself wherein the potential failure modes and its cause and effect on each component, assembly and subsystem can be studied to find out the best configuration. Although this is a very potent tool which can be applied during the design process, there isn't much literature available unlike the case of FDIR.

Background Review

Extensive research has gone into the fault detection, isolation and reconfiguration of control actuation systems in aircrafts and launch vehicles. Vedova et al. [2] proposed a simulated annealing-based fault identification algorithm for the prognosis of electromechanical actuator affected by multiple failures. Different levels of seizure and backlash were considered as fault detection parameters. Although this is a feasible technique for the prognosis in aircrafts and launch vehicle control systems, we need faster detection time and real-time reconfiguration techniques to overcome failures with severe effects. Belmonte et al. [3] proposed a model-based prognostic algorithm to identify precursors of incipient failures in primary flight control electromechanical actuators. Fault detection identification of an incipient failure is performed by analyzing the system parameters through a numerical algorithm based on spectral analysis. This method is used to detect the progress of a partial single-phase turn-to-turn short circuit in a motor along with the eccentricity of the rotor. A robust health monitoring system for EMA capable of early detection was conceived by Byington et al. [4]. A model-based method was used for the physical modeling along with advanced parametric identification techniques and failure prediction and detection algorithm to predict the time to failure for each of the critical failure modes within the system. The failure modes of direct drive EMAs can be identified such as channel jam, spalling, sensor bias, sensor drift and sensor scaling. Balaban et al. [5] designed a neural network-based diagnostic system which was generated based on the data obtained from experiments conducted in a test stand. Arriba et al. [6] designed an EMA with an anti-jamming device and implemented a health and usage monitoring system (HUMS) for the usage of EMA in safety-critical functions such as primary flight control systems. Mazzoleni et al. [7] detailed the project undertaken to design a more reliable EMA for aerospace system wherein the EMA was designed after conducting a thorough failure modes effect and criticality analysis and fault tree analysis. The EMA system uses new sensors, design solutions and a health monitoring capability that estimate the current health of the system and the residual useful life. Baklouti et al. [8] integrated the safety analysis in a model-based system approach wherein a preliminary FMEA is automatically generated from the system model and then recommendations are made to enhance the system design simultaneously complying with the safety requirements. Yao et al. [9] gave an accelerated test method for EMA to predict the life based on Wiener process degradation model. Electromagnetic clutch and tachogenerator which are considered as the weak elements of EMA are subjected to accelerated test by increasing the test frequency and changing the action time of the load, respectively. A control system for an EMA with advanced safety requirements was designed by Grepl et al. [10] based on FMEA which proposed two channel redundant structure of sensors and electronic control units. A voter implemented in complex programmable logic device using hardware description language (HDL) selects the healthy channel for the control. Zhu et al. [11] studied the reliability of EMAs having different architectures with and without jamming. Redundancy and fault tolerance were decided based on reliability, weight, control complexity and cost. Two anti-jamming EMAs with dual three-phase drives connected in parallel met the requirements of the safety-critical actuation requirements. Clausing et al. [12] gave a novel idea to improve the reliability by adopting failure mode avoidance technique in the conceptual design phase. The failure mode can be avoided by relaxing the constraint limit on uncoupled control factors, using physics of incipient failure to avoid failure, creating two distinct operating modes for two demand conditions and exploiting interdependence between two operating window system

variables. This approach is also used in the conceptual design of the actuator for the thrust vector control of a launch vehicle.

Objectives

1. To revisit the failures encountered in EMAs and look at their root cause analysis and preventive actions which can be considered for the new design.
2. To improve the fault tolerance of EMAs in two phases by providing redundancy to the electrical elements and then to the mechanisms.
3. To design an EMA following the failure mode avoidance technique through four strategies ensuring mistake avoidance and robustness in the design.
4. To conduct FMEA studies to ensure that the new actuator has reduced single failure points and provides better fault tolerance to its electrical elements and mechanisms.

System Description

Thrust Vector Control System

The thrust vector control of the terminal stage of a satellite launch vehicle developed by Indian Space Research Organisation (ISRO), named here as LV-A, has two electromechanical actuators. The orthogonally located linear actuators can move the engine about pitch and yaw axes (Fig. 1). The specification of thrust vector control system is shown in Table 1. There is no fault tolerance in the control actuation system for its electrical elements and mechanisms. This class of actuators is named as no redundancy actuator (NRA). Two configuration options are studied to introduce fault tolerance. One option is to provide fault tolerance for the electrical elements alone and maintain sufficiently high design margins in its mechanisms to keep the operating point well away from its failure limit. These actuators can be abbreviated as ERA (electrical redundancy actuator). The second option is to provide redundancy to the electrical elements and mechanisms through a concept named as high redundancy actuator (HRA).

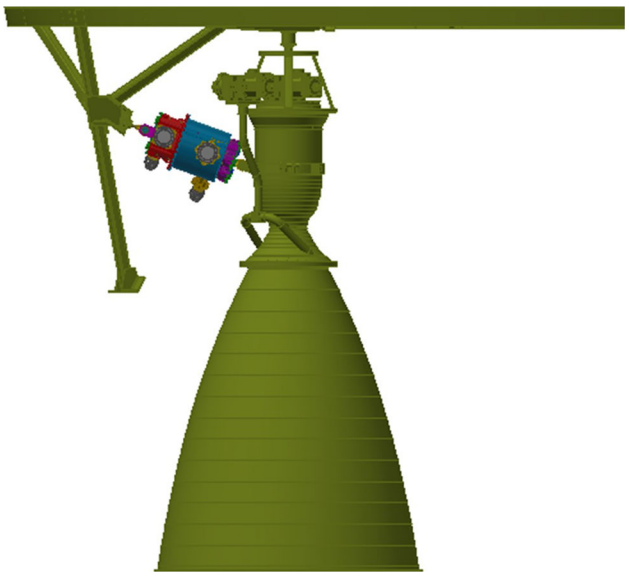

Fig. 1 Engine gimbal control system

No Redundancy Actuator (NRA)

A brush-type DC motor directly mounted on the ball screw is the prime mover (Fig. 2). The integral key at the end of ball screw which moves along a keyway does the rotary to linear conversion of the motion. Linear variable differential transducer (LVDT) which acts as the position feedback sensor is configured inside the hollow ball screw shaft. The LVDT probe is attached to one end of the moving ball screw shaft, whereas the LVDT having transformer windings is attached to the stationary part of the actuator.

The controller (Fig. 3) consists of a compensator, power amplifiers to power the motor windings in PWM mode, demodulator filter to convert the high-frequency AC signal from LVDT to DC signal, rate loop filter to generate the velocity signal from position signal, rate loop compensator, notch filter to attenuate the structural resonant frequency of the system and a current feedback loop. There is no redundancy to the controller and the batteries providing power to the power amplifiers.

Table 1 Specification of thrust vector control system

Parameter	Value	Unit
Thrust vector control	$\pm$ 2	°
Engine mass	100	kg
Mass M.I. of engine	13	kg m^2
Gain bandwidth (10%)	$>$ 4	Hz
Engine slew rate	10	°/s
Ball screw pitch	5	mm
Actuator moment arm	316	mm
Motor torque constant	0.18	Nm/A

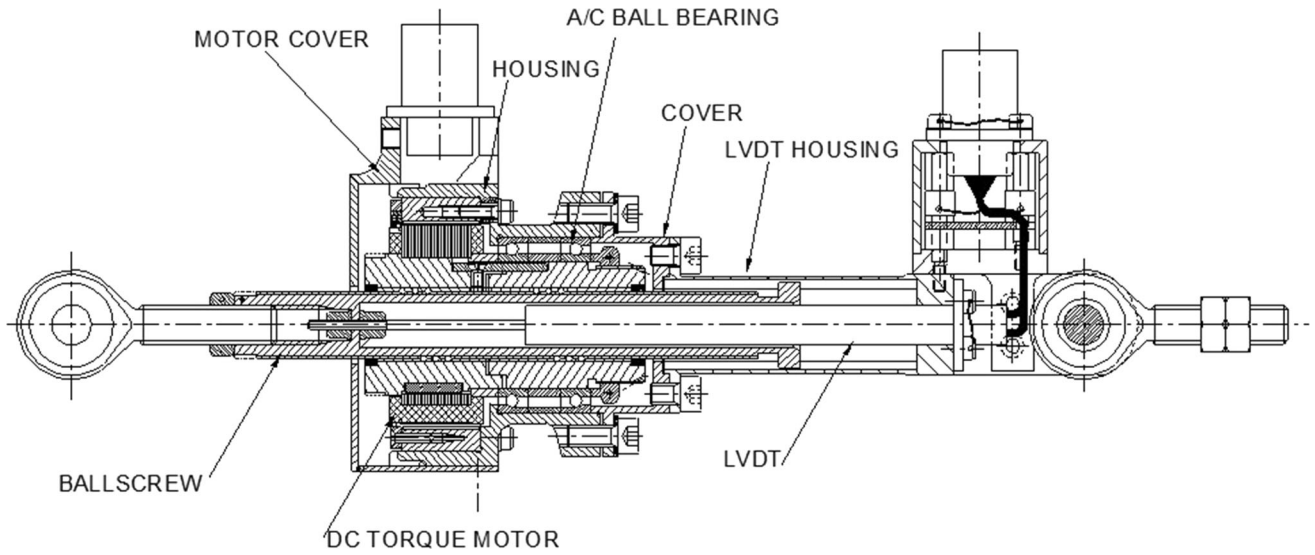

Fig. 2 No redundancy actuator

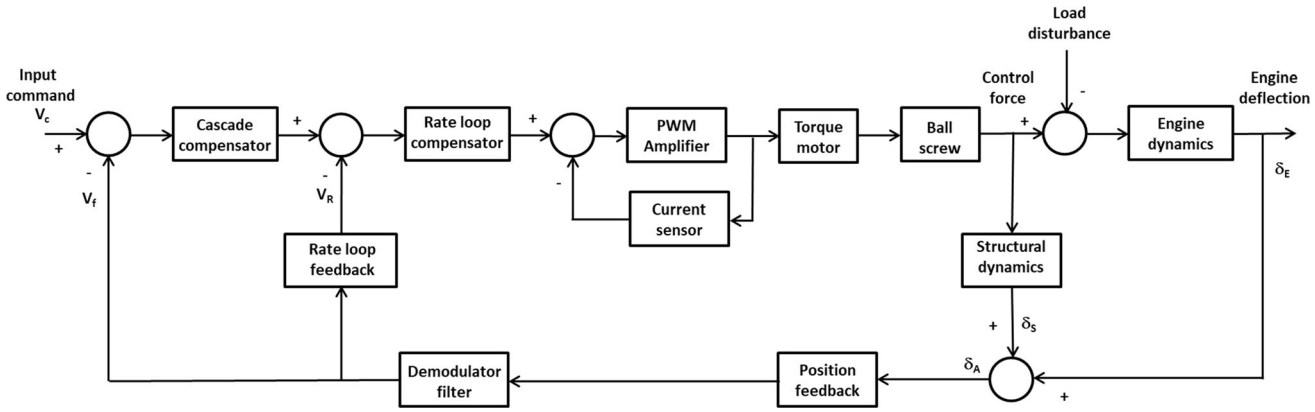

Fig. 3 Functional block diagram of NRA system

Failure Mode Investigation and Lessons Learned in EMA

When the failure modes and the failure mechanisms are well understood and actions are taken to avoid these failure modes, the system becomes more reliable. Hence, systems must be rigorously analyzed and tested for the failure modes. Hence, it is of paramount importance to brainstorm and understand and address the failure modes. Also, all the earlier failures encountered have to be analyzed and corrective actions were taken as explained by Elizabeth et al. [13]. In this section, the potential failure modes and their effects in mechanisms such as motors, ball bearings, ball screws, LVDTs and the preventive measures to be taken to reduce the chances of failure are addressed. Some of the failures during the development process and the corrective actions taken to avoid the recurrence in future hardware are also mentioned.

Ball Screws and Ball Bearings

Failure Reasons and Preventive Action

Higher than normal running torque is a commonly observed fault in ball screws and ball bearings. The probable causes can be,

1. A bend screw shaft and its misalignment with respect to journals, housing or slides.
2. Higher wear due to improper lubrication, incorrect lubricant selection and contamination in balls, tracks, races and lubricants
3. Adverse effect of lubricant on tracks and balls, improper wipers and cages in ball screws and bearings, respectively, absence of protective bellows in actuators, improper lubricant filters and wash away of lubricants during cleaning.
4. Corrosion, fatigue and excessive vibration levels.

5. Over load, improper heat treatment process which can result in a lower surface hardness and case depth, mismatch in lead between ball screw and nut, improper deflectors which are separately machined and assembled to the ball screw nut, operating at higher than the critical speeds and excessive preload applied on ball screws and bearings.
6. Increased backlash due to loss of preload, incorrect selection of contact angle for ball bearings, higher geometrical clearances with respect to housing and shaft, lower structural stiffness of bearing housing and increased play between the rotary to linear conversion mechanism.

Lessons Learned

During the acceptance testing of a ball screw lot, cracks were observed in certain number of ball screws near the shaft end (Fig. 4). The reason was found out to be the higher stress caused by tightening of M5 screws during the running-in test. Structural analysis confirmed that a radial force of 1000 N on the screw shaft end during the tightening of M5 screw leads to a tensile hoop stress of 330 MPa at the inner diameter which can initiate a crack that propagates through the thickness. Microstructure studies confirmed that the cracks initiated from the inner diameter location as concluded by the structural analysis. The root cause for the failure was attributed to the uncontrolled tightening torque applied on M5 screws to hold the fixture with respect to the ball screw shaft. The corrective action recommended to apply a controlled preload torque on M5 screws to maintain the stress within the acceptable limits.

Another failure was reported during the acceptance testing of an actuator, wherein the actuator output was not exactly following the command during which the motor current was slightly higher than the nominal value (Fig. 5). The anomalous behavior was found out to be due to the ball screw wiper made of felt material getting dislodged from the designated slot and coming out through the annular gap between the ball screw nut and the shaft. This caused higher resistive torque of ball screw leading to higher current and affecting the actuator output. The actuator output obtained from LVDT during a healthy state and wiper stuck condition are shown in Fig. 6. Had the wiper moved further into the ball track region, it would have led to either a partial stuck or fully stuck failure. The reason was attributed to the extra length of the open-ended wiper projecting out radially into the ball screw shaft (Fig. 7). The wiper design was changed from open type to a closed type made out through punching process as shown in Fig. 8. The lesson learned is that any uncontrolled dimension to a seemingly non-critical part can lead to a partial or complete failure. Hence, a strict dimensional control should be maintained for even non-critical parts such as wipers.

Motors

Failure Reasons and Preventive Action

Thermal fatigue can lead to insulation breakdown of motor windings. The permanent magnets can get demagnetized if they are exposed to a temperature above the critical temperature which depends on the type and shape of the magnet. There can be an increase in the motor current requirement due to the increased winding resistance which may worsen the situation. Hall effect sensors used for the electronic commutation of the motors are generally rated between 125 to 150 °C. Since these sensors are positioned close to the windings, the chances of temperature exceeding its limits are high. Hence, the temperature should always be maintained within the acceptable limits. Hall effect sensors are prone for electrostatic discharge (ESD) failures. In case, an electrostatic discharge strikes a powered Hall sensor, the failure signature will look like an electrical over stress (EOS), sometimes even showing

Fig. 4 Crack found through die penetrant test

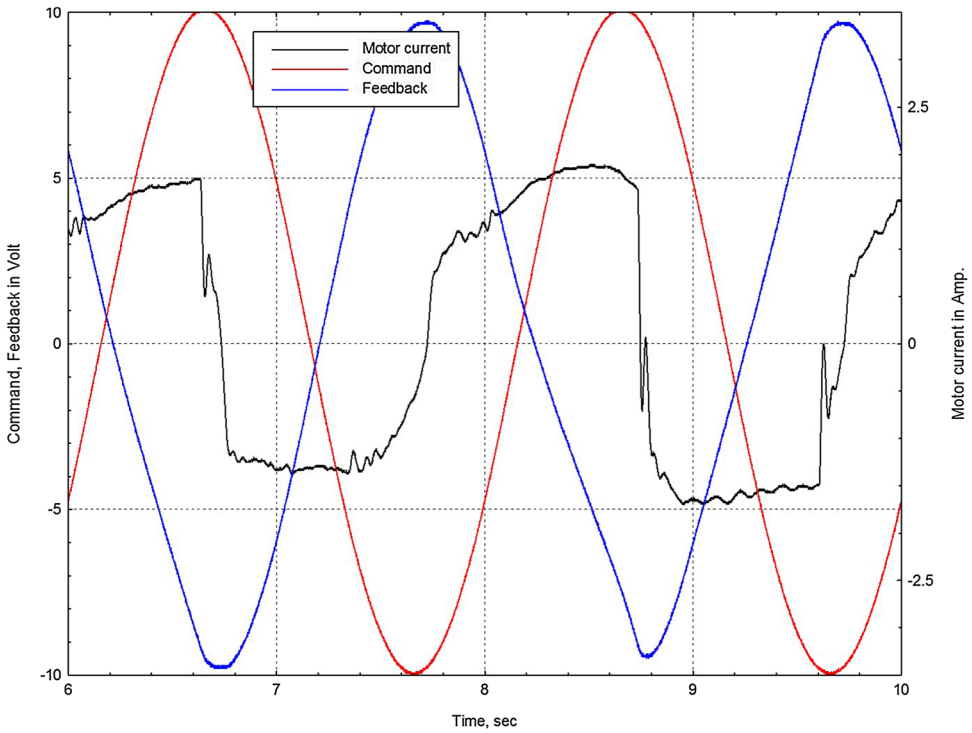

Fig. 5 Actuator output with wiper partially stuck

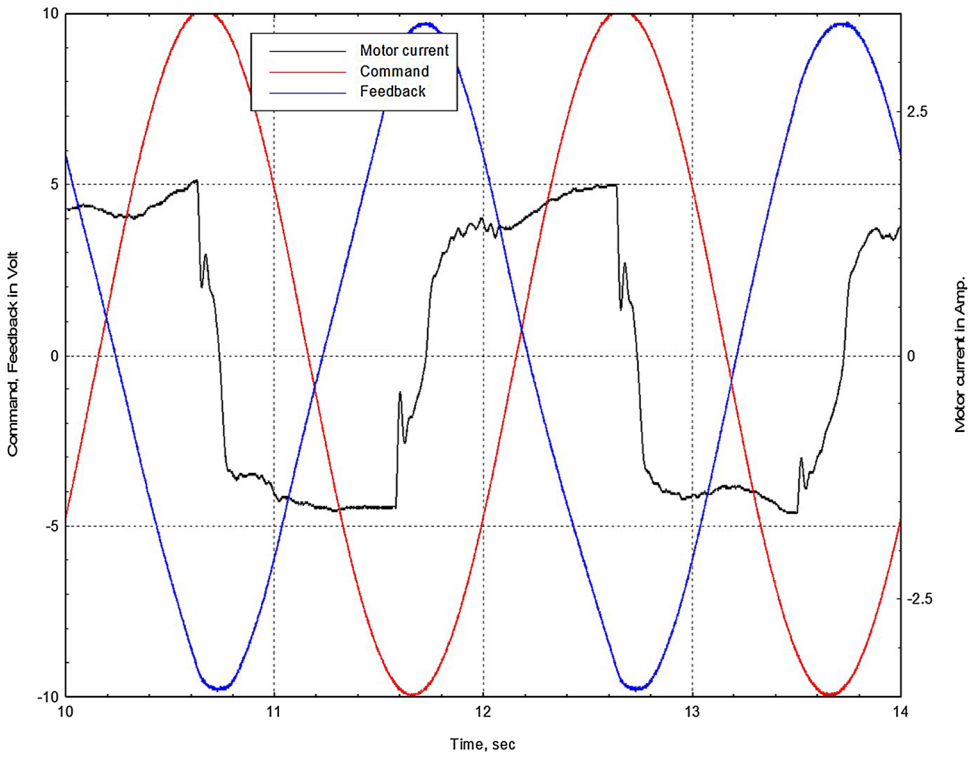

Fig. 6 Actuator output in healthy condition

several failure points where an ESD strike can turn on both p-channel and n-channel FET and create short from V_{dd} to V_{ss}. Hence, always the Hall sensors are handled with adequate ESD protection. Other failures can be due to the magnets flying off the high-speed rotor and degradation in insulation resistance due to ingress of moisture.

Fig. 7 Felt wiper partially dislodged and stuck

Fig. 8 Felt wiper design improvement

Lessons Learned

The rotor of a BLDC torque motor having permanent magnets was assembled to its stator through a manual process. During the insertion process, the rotor hit the inside surface of the stator leading to chipping of magnets (Fig. 9). This dislodged piece if unattended can get stuck in between the stator and rotor leading to either a partial stuck or a fully stuck condition. The corrective action was done by designing a new rotor insertion device which ensures concentric, guided and controlled entry of rotor to the stator, thereby avoiding any chance of rotor hitting the stator (Fig. 10).

Another failure encountered was the malfunction of a Hall sensor of a BLDC torque motor during the cold soak test of EMA. The BLDC motor had quadruplex sets of windings and Hall sensors for redundancy purpose. The dual redundant controller switched from prime channel to redundant channel at 13 °C. Further investigative tests revealed that the root cause was due to the intermittency in the excitation line to the Hall sensor (H_{BC}) of set-3 which

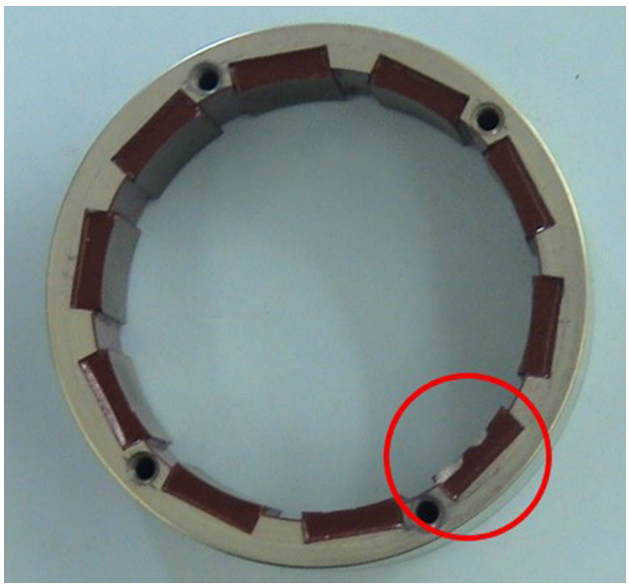

Fig. 9 Damaged rotor

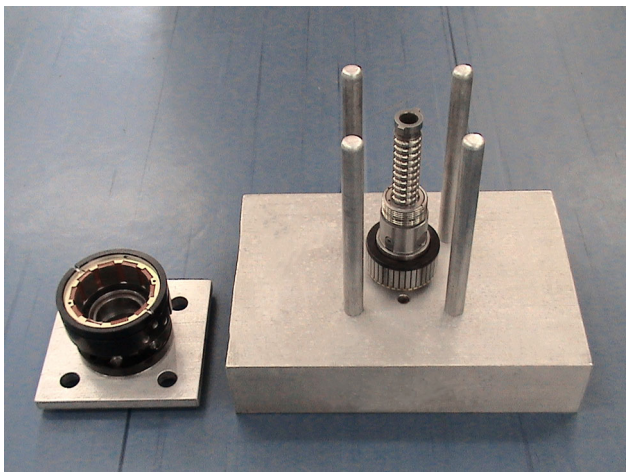

Fig. 10 Guided entry of stator to rotor

caused the output to be zero (Fig. 11). The intermittency was further traced to the dry solder joint of Hall sensor lead wire to the PCB. This was confirmed by the driving of motor through external excitation of Hall sensors bypassing the PCB inside the motor for which the potting compound had to be chipped off (Fig. 12). Spectroscopic analysis of the solder material revealed that the solder was lead free, which caused a dry solder joint. The microscopic analysis of the PCB found that the plated through hole (PTH) thickness was only around 12 microns as against the specification of greater than 25 microns. Due to the differential expansion during the cold soak, the electrical contact became intermittent leading to the detection of Hall sensor fault. The corrective action was to adopt a better soldering process to avoid dry solder, usage of liquid flux

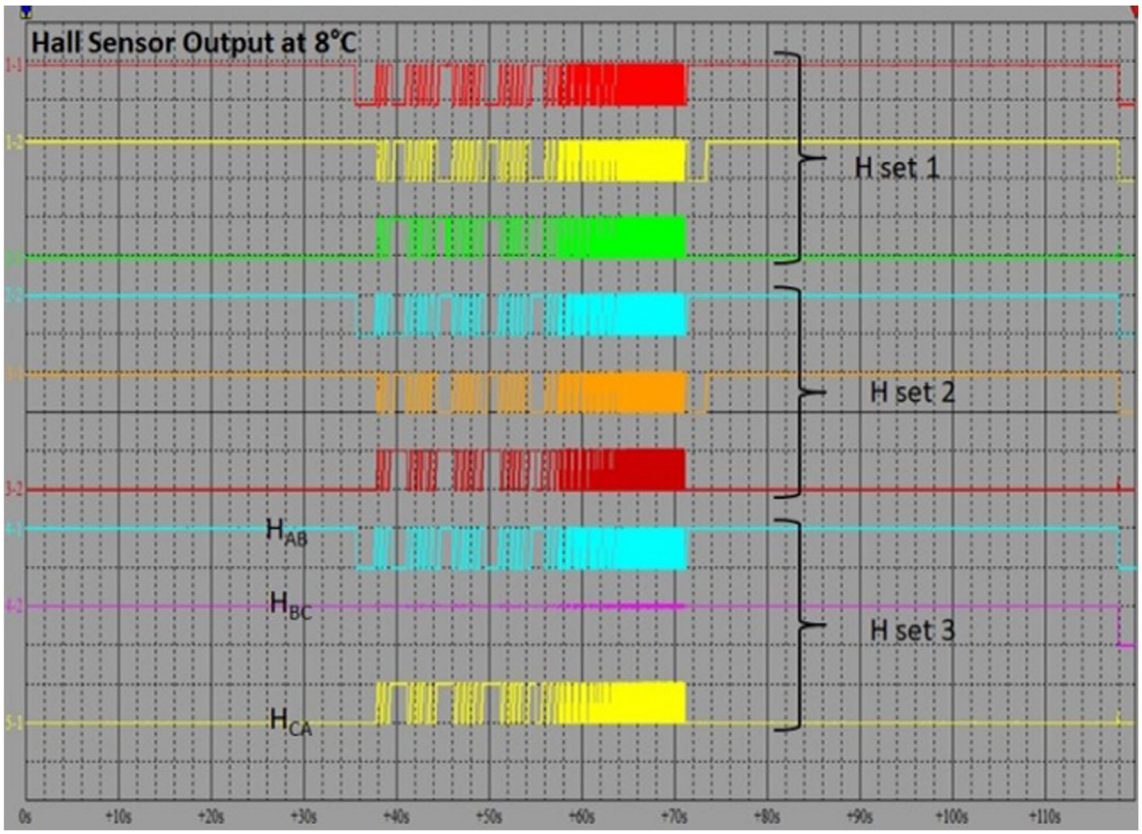

Fig. 11 Failed Hall sensor output (H_{BC} of set 3) at 8 °C

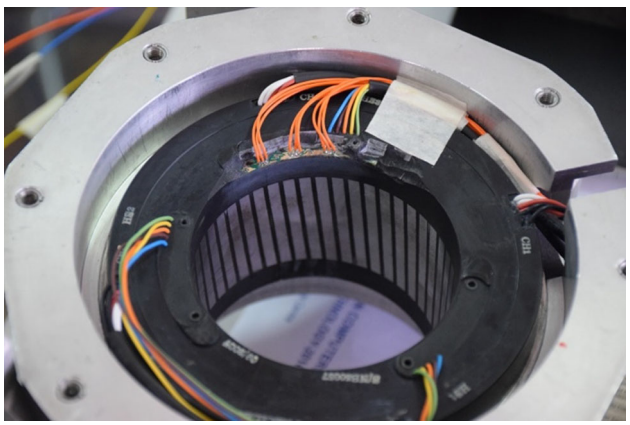

Fig. 12 BLDC motor with bypass circuit

to avoid oxidation build-up in copper and solder and to increase the plated through hole thickness of PCB.

LVDT

Failure Reasons and Preventive Action

LVDTs are more reliable compared to conductive plastic track potentiometers. However, LVDTs are prone to failure in certain critical and demanding applications characterized by high temperatures, excessive radiation and heavy shock and vibration. The long probe which is structurally analogous to a cantilever beam can fail if the stress exceeds the limiting value during conditions such as vibration and shock. An open primary winding will cause a zero differential voltage between the two secondary windings which is the center position for most of the actuators. An open failure in either of the secondary windings will force the LVDT output to the extreme positions of the output shaft. Thermal drift beyond the specified value is a common mode of failure which can be overcome by the usage of ratiometric LVDTs wherein the secondary voltages are available separately. Loss of insulation resistance is another commonly observed failure mode which can be avoided by hermetic sealing of the sensor or the actuator.

Lessons Learned

During the EMI test of actuator for the RS02 levels, the actuator motor current got abnormally increased to 1.7A as against the nominal value of 0.3A without any increase in the external load (Fig. 13). The root cause was the electromagnetic coupling of the external field generated through 20A, 50 Hz supply according to the RS02 test

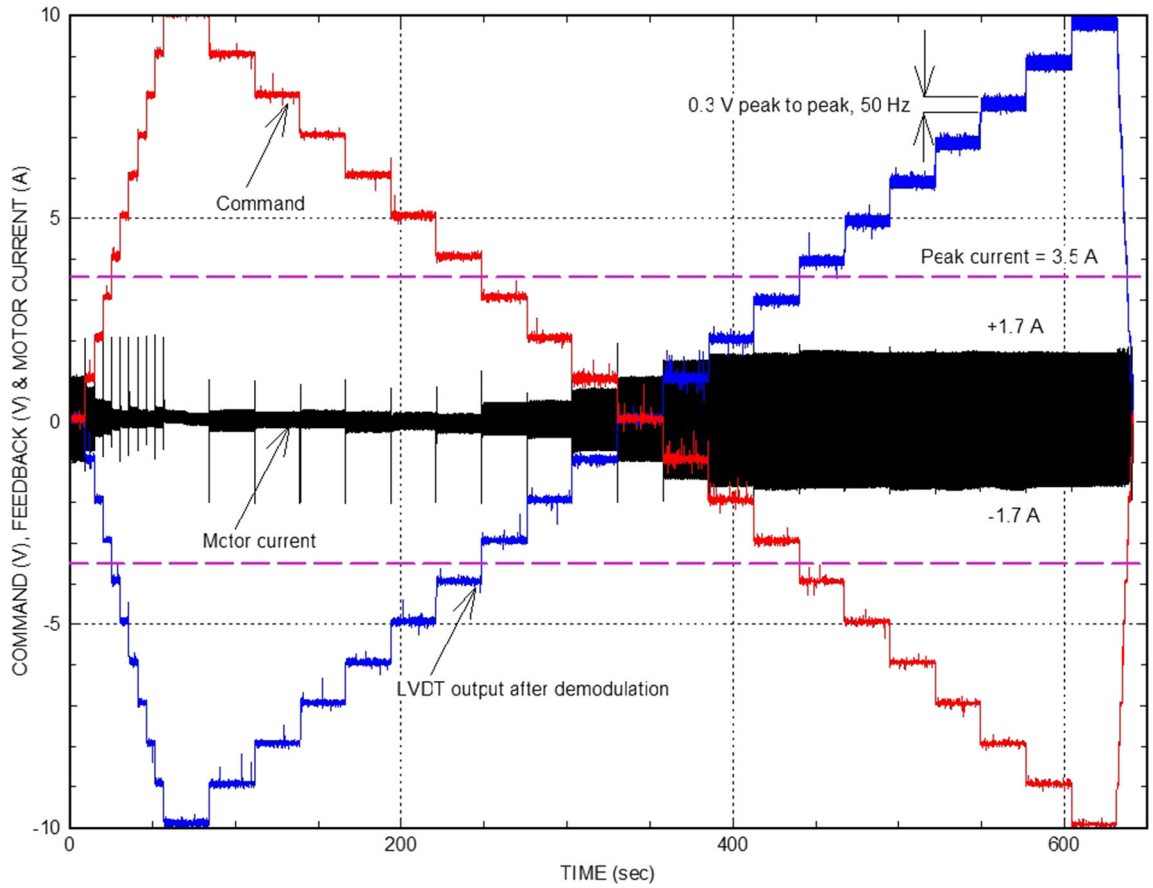

Fig. 13 Actuator output with poor shielding

requirement. The high frequency variation in the LVDT output affected the error signal of the closed loop position control system which in turn led to the higher current demand for the actuator motor. The EMI shielding design of the LVDT was found to be unacceptable and a better shielding scheme was implemented subsequently (Fig. 14).

In another application, the LVDT mounting M5 thread interface had failed. Investigation revealed that the thread was made of a hollow shaft, which was not apparently visible from outside. This caused high local stresses due to the reduced cross-sectional area, eventually leading to a tensile failure. This brought out the requirement of better understanding of internal features of the standard bought-out parts to avoid failures (Fig. 15).

Electrical Redundancy Actuator (ERA)

Most of the actuation systems used in expendable satellite launch vehicles does not have fault tolerance. There is a need to provide fault tolerance to the critical elements of the actuator. The first method is to introduce fault tolerance to the electrical elements of the actuator and the controller. The electrical elements consist of compensator, power amplifier, commutation logic circuits, current loop, feedback loop of the controller, batteries, motor and position sensors such as LVDT and Hall effect sensors. Three-phase BLDC motor is used instead of brush-type DC motor due to better life, reliability and torque-to-inertia ratio. The motor has dual three-phase winding, each configured in the 180 ° segment of the stator for physical isolation (Fig. 16). This ensures that any failure by means of short circuit will not migrate to the other channel. There are two sets of Hall effect sensors, each set driving one three-phase winding. Triplex LVDTs are used to sense the actuator movement to close the feedback loop

The controller has dual redundancy wherein LVDT-1 closes the loop of controller 1 and LVDT-2 that of controller 2 (Fig. 17). By default, the system works using controller 1 and in case of a failure, the control will switch over to controller 2. To detect the failure in controller 1, analytical redundancy is employed using a mathematical model which generates a simulated position output. This output is compared with the output of LVDT-3 and in case

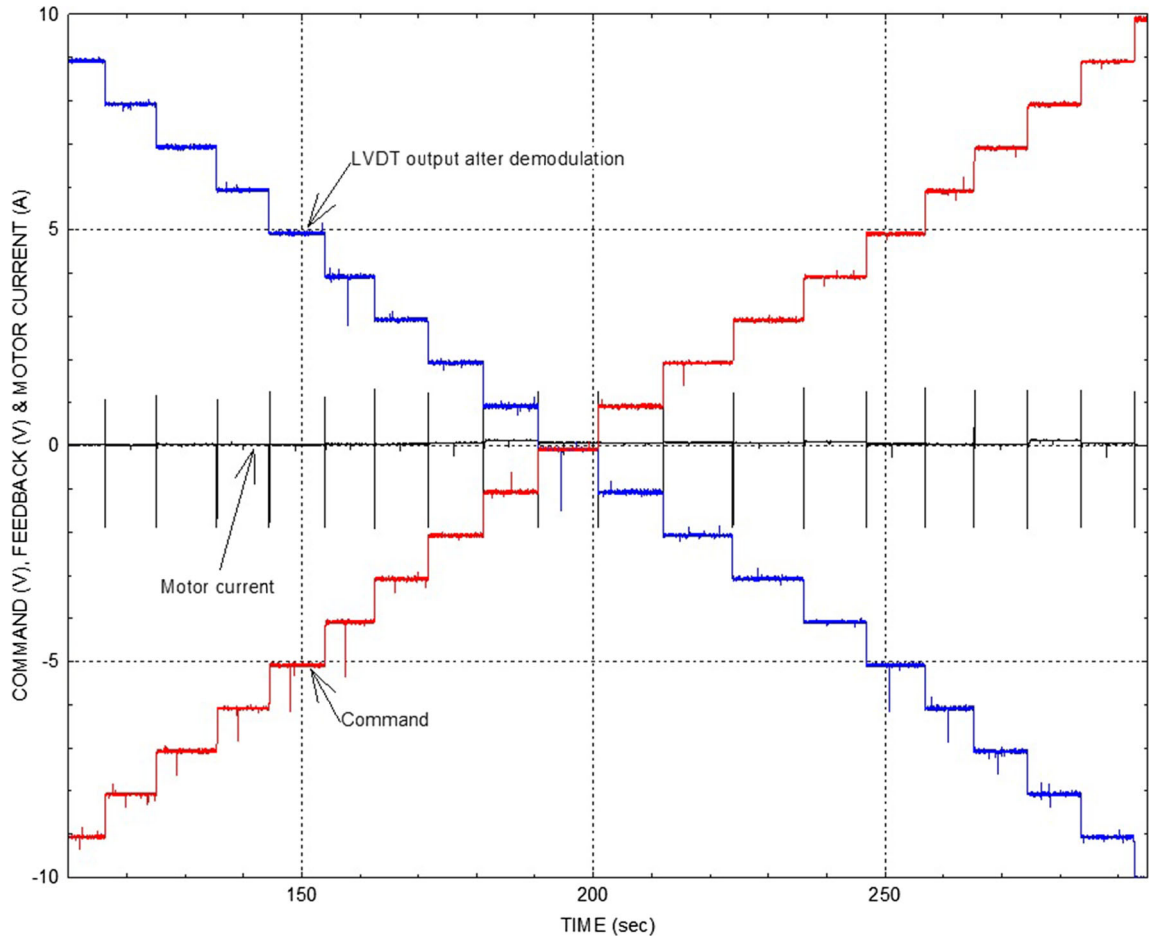

Fig. 14 Actuator output with improved shielding

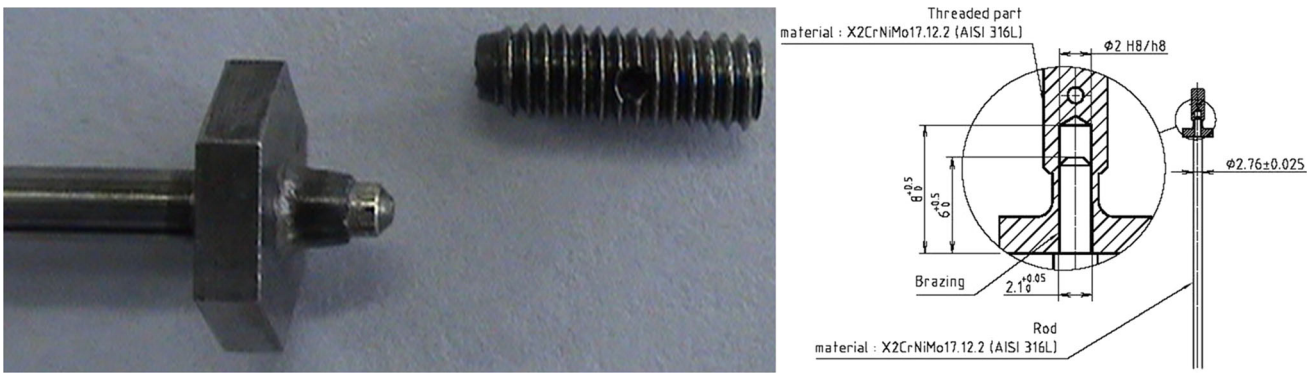

Fig. 15 LVDT thread failure

the difference goes above a certain threshold value, the control will switch over from controller 1 to controller 2. Separate power amplifiers drive each motor through separate current commands. Even if one power amplifier fails, it will incapacitate only one coil of the motor, thereby reducing the force capability to 50% of the maximum capacity. Hence, the motors are selected with two times the maximum torque requirement.

High Redundancy Actuator (HRA)

This is a new concept for the health management of electromechanical actuators without the need for a complex fault detection isolation and reconfiguration scheme. The motivation and principle are derived from musculature, wherein the micromovement of individual muscle units is combined to produce a macromovement. The damage of an

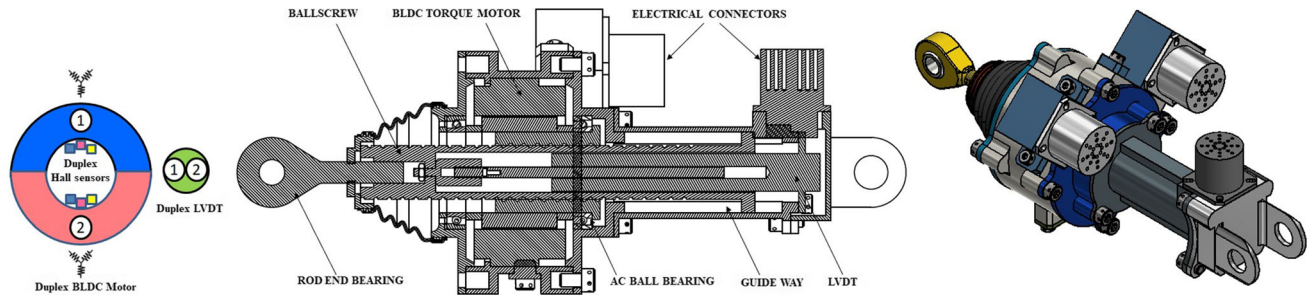

Fig. 16 Electrical redundancy actuator

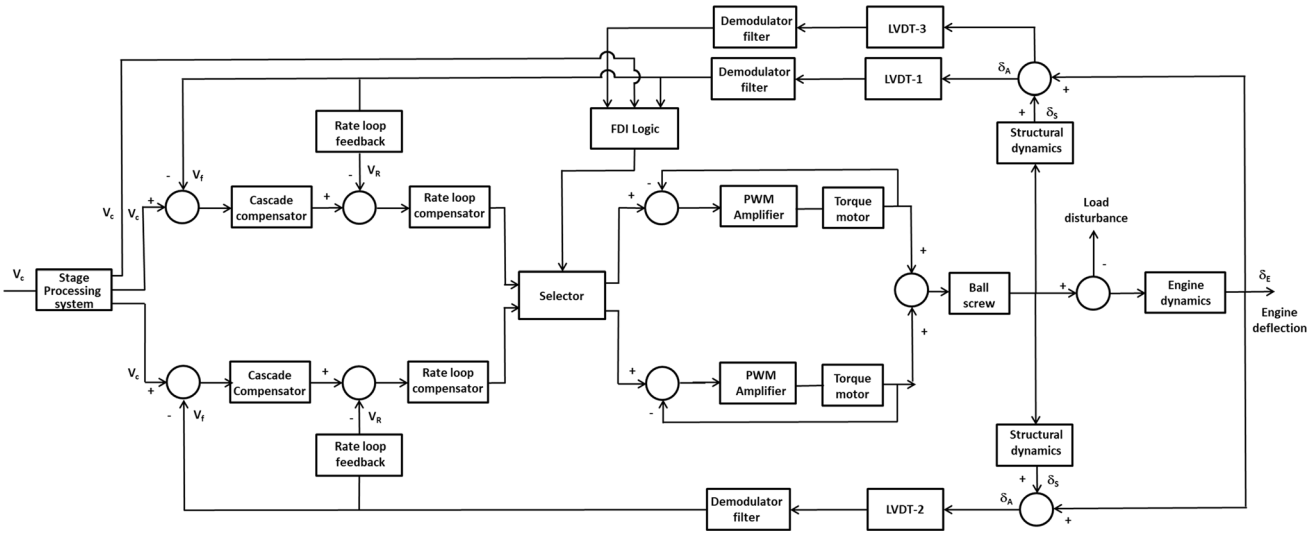

Fig. 17 Functional block diagram of ERA system

individual cell or a few of them will not have a considerable effect on its functioning. In a high redundancy electromechanical actuator, a number of microactuators are configured in a series–parallel combination to mimic the property of musculature. Dixon et al. [14] demonstrated the feasibility of the HRA concept by showing that a highly redundant actuator in 2 × 2 configuration, comprising a relatively larger number of actuation elements, can be controlled in such a way that faults in individual elements are inherently accommodated, although some degradation in overall performance will inevitably be found. The number of actuators in series–parallel configuration affects the tolerance to failures of individual units. Stuck failure of a single actuator blocks the output motion of other microactuators in parallel, thereby reducing the overall stroke of the actuator. A loose failure to one microactuator reduces the overall force capability of actuator by a fraction of the number of actuators in parallel. Hence, the actuator needs to be overdesigned for the stroke and force requirement to tolerate stuck and loose failures. The required control performance can be obtained through a robust control structure without any reconfiguration mechanism.

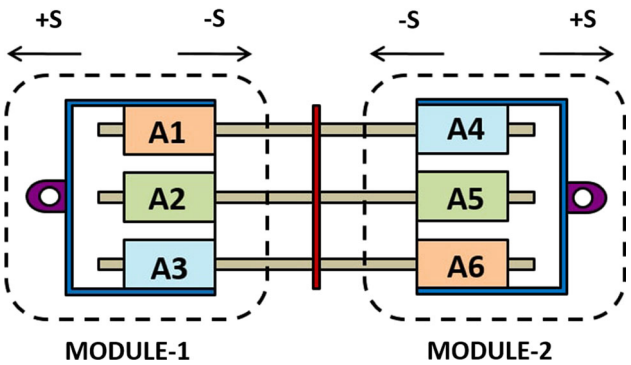

Fig. 18 HRA in 3P2S configuration

Prasad et al. [15] showed the design and feasibility of using electromechanical actuators in high redundancy configuration for the thrust vector control application in the terminal stage of a satellite launch vehicle. A high redundancy actuator in 3P2S configuration has two modules in series wherein each module has three microactuators joined in parallel (Fig. 18). Each microactuator is a direct drive

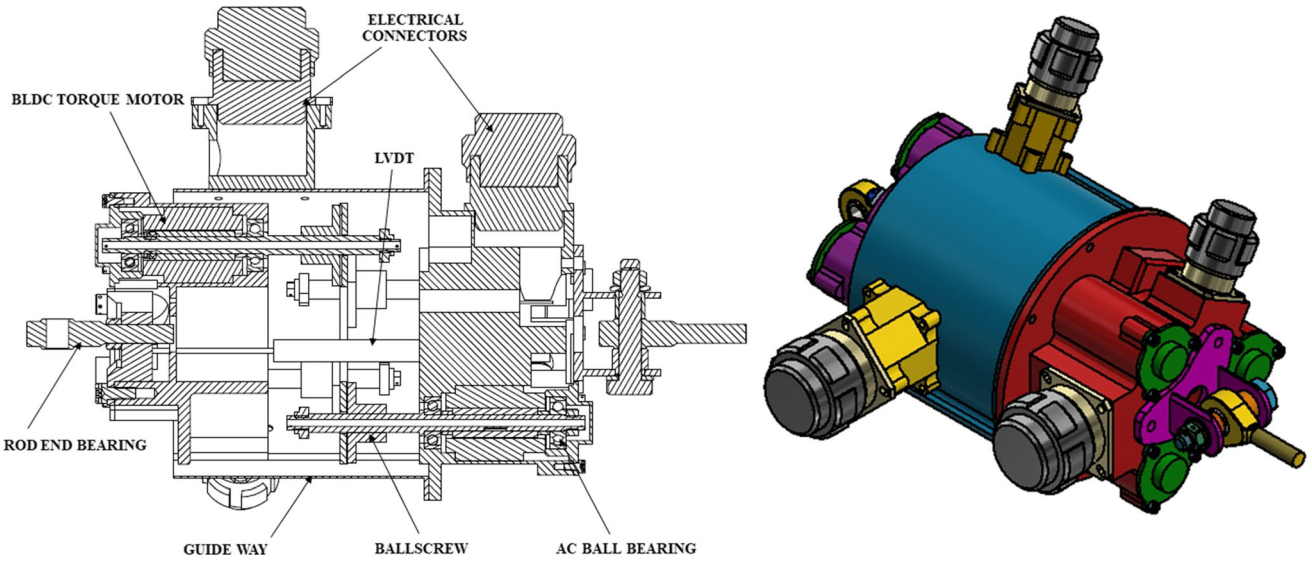

Fig. 19 High redundancy actuator

linear electromechanical actuator, wherein the brushless dc torque motors directly drives the ball screw shaft. Hall effect sensors provide the commutation logic for the three-phase BLDC motor. The motor stator is assembled in such a way that the back emf of all the three motors of each module is synchronized. This can be achieved by rotating the stator of two motors in each module and locking them when the back emf matches with the third motor. The ball screw shaft is supported by two angular contact ball bearings on either end. The ball screw nuts are attached to a common central plate which converts the rotary to linear motion. Two rod end spherical bearings on either side of the actuator connect it to the engine and stage sides. The combined motion of all microactuators results in the increase or decrease of the actuator length which is sensed by the three LVDTs (Fig. 19). There are two controllers out of which the first one will drive the actuator based on the output from the first LVDT. The output of second LVDT is connected to the second controller. The output of the third LVDT is compared with the output of a mathematical model on real-time basis to detect the fault. In case of fault detection, the reconfiguration is done by switching the controller from the first to the second one. For this configuration, a single failure to LVDT, Hall sensor, motor winding, drive controller, ball screw or a ball bearing will not lead to a complete failure. Instead, there will be a graceful degradation in actuator performance which can be demonstrated through simulations and testing. The controller has dual redundancy wherein LVDT-1 closes the loop of controller 1 and LVDT-2 that of controller 2 (Fig. 20). By default, the system works using controller 1 and in case of a failure, the control will switch over to controller 2. To detect the failure in controller 1, analytical redundancy is employed using a mathematical model which generates a simulated position output. This output is compared with the output of LVDT-3 and in case the difference goes above a certain threshold value, the control will switch over from controller 1 to controller 2. There are three current loops and three power amplifiers, each driving one motor of each module. All six motors are driven through a common current command. The current command is the average of six current sensor feedbacks. Hence, even if one power amplifier fails, it will incapacitate only one motor of each module, thereby reducing the force capability to 66.7% of the maximum capacity. In case of a stuck failure to any mechanical component such as motor, ball bearing and ball screw, the stroke reduces to 50%. For a loose failure to one component, the force capability reduces to 66.7%. Hence, the motors are selected with 1.5 times the maximum torque requirement and the stroke capability of each microactuator is equal to the maximum requirement. Even under a stuck failure in any mechanical component, HRA will have the maximum stroke capability.

Design for Failure Mode Avoidance

In the traditional formulation, reliability is defined as the probability that a product or system will perform its intended function adequately for a specified period of time in a defined environment. To compute the reliability of a product, we need to know the survival function, failure rates of the individual components and mean time between failures. The failure rate of the new product can be estimated only if all the above data are available. Reliability also requires two critical conditions which are mistake

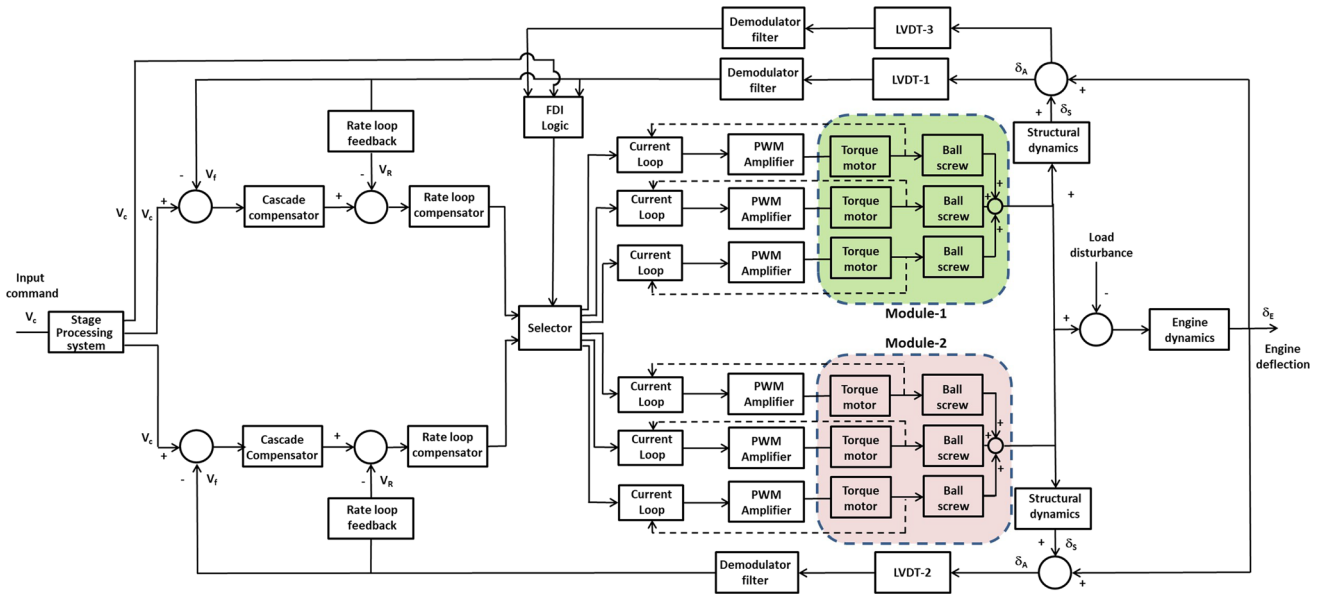

Fig. 20 Functional block diagram of HRA system

avoidance and robustness [12]. 'Mistake' refers to the wrong decisions taken during the design stage and wrong operations during the manufacturing process. 'Robustness' indicates the ability of the system to function under a healthy manner under the full range of conditions that may be experienced in the operating field. In the design stage of EMA, this alternate concept called "failure-avoidance' is used to arrive at the final design configuration. Clausing et al. suggested that the most significant improvements in reliability come in the system design stage by moving the physical failure modes. The four strategies for improved robustness are applied in the design of HRA.

The first strategy is to relax a constraint limit on an uncoupled control factor. The constraint limit for the NRA and ERA is the continuous rating of actuator based on the thermal design margins. One of the main reasons inhibiting the usage of EMAs in primary flight control system is the continuous aerodynamic load and the corresponding thermal effects on the actuator. The continuous rating is constrained by the maximum permissible winding temperature decided by the insulation class. This was improved through a decentralized architecture of motors wherein the total thermal energy due to the copper losses gets distributed in six different locations of motors, thereby increasing the continuous rating. Another constraint limit was on the self-inertia of the actuator rotor which consists of motor rotor, ball screw and ball bearing. Through a distributed architecture, the total self-inertia was reduced by one order [14]. This has also increased the design margins of the actuator and moved the operating point away from the limiting power levels. The second approach is to use physics of incipient failure to avoid failure. In

Table 2 Ranking system to find CN

Number	Severity number (SN)	Probability number (PN)	Detection number (DN)
1	Negligible	Extremely remote	Very likely
2	Major	Remote	Likely
3	Critical	Occasional	Unlikely
4	Catastrophic	Probable	Extremely unlikely

many cases, the failure mode exhibits distinct phenomenon after the onset of the failure mode is approached. There is no fault tolerance to the position feedback sensor in NRA. In HRA, the three LVDT outputs are compared with a mathematical model output to identify the faulty output and isolate it from further usage. In this way an incipient failure is avoided through a fault detection isolation and recovery logic. The third strategy is to employ two different operating modes. This approach is followed when the development process reaches a state in which the system has a limited operating window between multiple one-sided failure modes and therefore cannot operate reliably. In such cases, it is advisable to change from single operating mode to two operating modes. If any mechanism of NRA such as ball screw, ball bearing, or motor fails in a stuck or loose mode, it will lead to a total failure of the actuator system. In case of HRA, for a single stuck failure, the total actuator force reduces to 66.7% and the speed reduces to 50%. The controller has the intelligence to sense the failure condition and through a compensator gain boosting technique it makes the system to perform within the specified bounds. The fourth strategy is to identify and

Table 3 Criticality Number of motor

No.	Failure Mode	Effect	Severity			Occurrence			Detection			RPN		
			NRA	ERA	HRA	NRA	ERA	HRA	NRA	ERA	HRA	NRA	ERA	HRA
1	Continuity loss in one coil	Loss of motor power leading to control loss	4	1	1	1	1	1	1	1	1	4	1	1
3	Loss of Insulation resistance	Leakage current leading to lower output power	2	1	1	1	1	1	1	1	1	2	1	1
4	Brush wear	Total wear can lead to loss of commutation and no rotation of motor	4	-	-	1	-	-	1	-	-	4	-	-
5	Brush de-bond	No commutation and rotation of rotor	4	-	-	2	-	-	2	-	-	16	-	-
6	Loss of stiffness in Be-Cu strip	Intermittent brush contact affecting commutation	4	-	-	2	-	-	2	-		16	-	-
7	One Hall sensor failure	No commutation and rotation of rotor	-	1	1	-	1	1	-	1	1	-	1	1
8	Hall sensor PCB failure	No commutation and rotation of rotor	-	4	-	-	1	-	-	1	-	-	4	-
9	One Hall sensor Excitation failure	No commutation and rotation of rotor	-	1	1	-	1	1	-	1	1	-	1	1
10	Magnet de-bond	Broken magnet chips can get stuck and hinder rotor motion resulting in lower motor output power	4	4	1	1	1	1	2	2	1	8	8	1
11	Magnet breakage	Single broken magnet can get stuck and hinder rotor motion resulting in lower motor output power	4	4	1	1	1	1	2	2	1	8	8	1

exploit dependencies among failure modes. The two-channel three-phase windings in BLDC motor of ERA can be wound in different ways. The straightforward way is to run both the channels in parallel throughout the stator slots. In this case any failure to the either channel can migrate to the second channel positioned in the close proximity. This mode of failure makes the redundant channel useless due to the interdependency of the first and second failures. This was overcome by designing an eight-pole BLDC motor having 24 stator slots for ERA wherein the two three-phase windings were physically isolated by positioning it in each halves of the stator. Two diametrically opposite teeth provide a physical separation. In this way, the interdependency of the failures was avoided. In HRA

Table 4 Criticality Number of position sensor (LVDT/Potentiometer)

No.	Failure Mode	Effect	Severity			Occurrence			Detection			RPN		
			NRA	ERA	HRA	NRA	ERA	HRA	NRA	ERA	HRA	NRA	ERA	HRA
1	Excitation failure of one sensor	No output from sensor leading to mission failure	4	1	1	2	2	2	1	1	1	8	2	2
2	Probe detachment of one sensor	No active sensing of position leading to mission failure	4	4	1	1	1	1	2	2	1	8	8	1
3	Intermittent loss of contact with conductive plastic track	Change in position feedback leading to change in vehicle attitudes and rates	-	3	-	-	2	-	-	2	-	-	12	-
4	Coil / track Continuity loss	No output for LVDT	4	1	1	1	1	1	1	1	1	4	1	1
5	Coil / track Isolation loss	Erroneous sensor output	4	4	1	2	2	2	1	1	1	8	8	2

Table 5 Criticality Number of ball screw/ball bearing

No.	Failure Mode	Effect	Severity			Occurrence			Detection			RPN		
			NRA	ERA	HRA	NRA	ERA	HRA	NRA	ERA	HRA	NRA	ERA	HRA
1	Spalling / Brinelling	Increased vibration	2	2	1	1	1	1	1	1	1	2	2	1
2	Contamination entering ball track area of one element	Partial or full stuck condition	4	4	1	2	2	1	1	1	1	8	8	1
3	Loss of preload in one element	Nonlinear input to output relation due to backlash	3	3	1	1	1	1	1	1	1	3	3	1

configuration, by virtue of the distributed architecture the interdependency of failures was avoided.

FMEA of Actuation System

The design FMEA supports the design process in reducing the risk of failures through an objective evaluation of design requirements and design alternatives, performing an initial design for manufacturing and assembly requirements, carrying out a design identifying the potential failure modes and their effects on the system, to design an efficient test and development programs, ranking the potential failure modes and prioritizing the design improvements and to provide an open issue format for recommending and tracking risk reducing actions. The potential failure modes and the effects are listed first. A severity number ranging between 1 and 4 is assigned for each of the potential failure mode, which is an indication of the seriousness of the effect. Then, an estimate is made on the likelihood of occurrence of each of the potential failure mode on a 1 to 4 scale. An assessment on the ability to detect and correct each failure is addressed through a detection number scaled between 1 and 4 (Table 2).

Finally, a Criticality Number (CN) ranging between 1 and 64 is found for each of the failure mode which is the product of Severity, Probability and Detection ranking

Table 6 Criticality Number of Controller

No.	Failure Mode	Effect	Severity			Occurrence			Detection			RPN		
			NRA	ERA	HRA	NRA	ERA	HRA	NRA	ERA	HRA	NRA	ERA	HRA
1	One compensator failure	Loss of control in the connected control chain	4	1	1	1	1	1	1	1	1	4	1	1
2	One Power amplifier drive failure	Loss of motor torque in the connected control chain	4	2	2	1	1	1	1	1	1	4	2	2
3	One LVDT demodulator failure	Wrong position sensing from LVDT	4	1	1	1	1	1	1	1	1	4	1	1
4	One current sensor failure	Affects the torque generated in the connected chain	4	2	2	1	1	1	5	1	1	4	2	2

[16]. CN for the failure modes in motor, position sensor, ball screw and controller are found (Table 3, 4, 5, 6) for the No Redundancy Actuator, Electrical Redundancy Actuator and High Redundancy Actuator. For higher CNs the design team took efforts to reduce the calculated risk through corrective actions.

There is a progressive reduction in the criticality number (CN) for all the failure modes envisaged in EMA due to the design improvements made in ERA and HRA. The improvement was very significant for ERA due to the usage of a brushless motor. Usage of multiple motors, ball screws and ball bearings avoided the stuck failure for HRA. By providing redundancy to the position feedback sensor, CN was reduced for ERA and HRA. Usage of multiple probes for the position feedback sensor in HRA eliminated the single failure point present in NRA and ERA. The dual redundancy provided in the controller improved the fault tolerance in ERA and HRA.

Conclusion

The Failure Mode Effects and Analysis of the electromechanical actuator used in the thrust vector control system of a satellite launch vehicle has been carried out. The root cause analysis and preventive measures identified for the previous failures in EMAs were considered in the new design of a fault tolerant EMA. The fault tolerance capability of EMA was improved in two stages; first by incorporating redundancy in its electrical elements and then by introducing fault tolerance for the mechanisms through the high redundancy actuator concept. The fault tolerance of EMA was improved through a design following four strategies under the failure mode avoidance technique. From the criticality number found out through FMEA studies conducted on three different configurations of EMAs, it can be concluded that the HRA configuration shows the highest fault tolerance.

Future work includes the reliability computation of the EMA and its controller for the three types of systems. Tests should be conducted on hardware by simulating stuck and loose failures using an external brake connected to the ball screw shaft. The acceptability of EMA in HRA configuration for the thrust vector control of a launch vehicle should be ensured through vehicle level simulation studies conducted in the presence of faults in its electrical elements and mechanisms.

Acknowledgment The authors wish to thank Director, VSSC, for the constant encouragement for advancement in the field of electromechanical actuation systems and permitting to publish the paper. The author gratefully acknowledges the critical review and comments on the paper by Mr. K.C. Reghunatha Pillai of Vikram Sarabhai Space Centre.

References

1. Guan Qiao, Geng Liu, Zhenghong Shi, Yawen Wang, Shangjun Ma, Teik C Lim, A review of electromechanical actuators for More/All Electric aircraft systems. J Mech Eng Sci **232**(22), 4128–4151 (2018)
2. M.D.L. Dalla Vedova, D. Lauria, P. Maggiore, L. Pace, Electromechanical actuators affected by multiple failures: a simulated-annealing-based fault identification algorithm. Int J Mech **10**, 219–226 (2016)
3. D. Belmonte, M.D.L. Dalla Vedova, C. Ferro, P. Maggiore, Electromechanical actuators affected by multiple failures:

prognostic method based on spectral analysis techniques, in Klimis Ntalianis, (Ed.), AIP Conference Proceedings, Vol. 1836 (Rome), pp. 020020-1–020020-6 (2017)
4. C. S. Byington, P.E. Paul Stoelting, A Model-Based Approach to Prognostics and Health Management for Flight Control Actuators, IEEE Aerospace Conference Proceedings, Vol. 6, 2004 (Montana), pp. 3551-3562
5. E. Balaban, A. Saxena, P. Bansal, K. F. Goebal, P. Stoelting, S. Curran, A Diagnostic Approach for Electro-Mechanical Actuators in Aerospace Systems, IEEE Aerospace Conference, 2009 (Montana), pp. 1–13
6. A. G. Ricardo de Arriba, Health and Usage Monitoring System (HUMS) Strategy to enhance the Maintainability & Flight Safety in a Flight Control Electromechanical Actuator (EMA). Third European Conference of the prognostics and health management society, Vol. 7, 2016 (Bilbao)
7. M. Mazzoleni, Y. Maccarana, F. Previdi, G. Pispola, M. Nardi, F. Perni, S. Toro, Development of a reliable electro-mechanical actuator for primary control surfaces in small aircrafts, International conference on advanced intelligent mechatronics, 2017 (Munich), pp. 1142–1147
8. A. Baklouti, N. Nguyen, F. Mhenni, J.-Y. Choley, Improved Safety Analysis Integration in a Systems Engineering Approach. J Appl Sci **9**, 1246 (2019)
9. N. H. J. Yao, S. Li, Accelerated Life Test and Life Prediction of an Electromechanical Actuator, in International conference on artificial intelligence and advanced manufacturing, 2019 (Dublin), pp. 647–651
10. R. Grepl, M. Matejasko, M. Bastl, F. Zouhar, Design of a Fault Tolerant Redundant Control for Electro Mechanical Drive System, Proceedings of the 21st International conference on automation & computing, 2015 (Glasgow), pp. 1–6
11. S. Zhu, T. Cox, Z. Xu, C. Gerada, C. Li, Design Considerations of Fault-Tolerant Electromechanical Actuator Systems for More Electric Aircraft (MEA). IEEE Energy conversion congress and exposition, 2018 (Portland), pp. 4607–4613
12. Don Clausing, Daniel D. Frey, Improving System Reliability by Failure-Mode Avoidance Including Four Concept Design Strategies. Syst Eng **8**(3), 245–261 (2005)
13. E. L Morse, J. R Fragola, B. Putney, Modeling launch vehicle reliability growth as defect elimination, in AIAA Space 2010 conference and exposition, 2010 (California)
14. X. Du, R. Dixon, R.M. Goodall, A.C. Zolotas, Modeling and control of a high redundancy actuator. Mechatronics **20**(1), 102–112 (2010)
15. B. Biju Prasad, N. Biju, M.R. Radhakrishna Panicker, High redundancy electromechanical actuator for thrust vector control of a launch vehicle. Aircraft Eng Aerosp Technol **91**(8), 1122–1132 (2019)
16. European Cooperation for Space Standardization (ECSS-Q-ST-30-02C): Space product assurance - Failure modes, effects (and criticality) analysis (FMEA/FMECA), ESA Requirements and Standardization Division, The Netherlands